IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: McGarvey et al.
Serial No.	: 09/921,536
Filed	: August 03, 2001
Title	: Methods, Systems and Computer Program Products For Secure Delegation Using Public Key Authorization
Attorney Docket	: 5577-236 (RSW920000185US1-IBM 019 PA)
Examiner	: M. Henning
Art Unit	: 2131
Confirm	: 6803

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

DECLARATION OF PRIOR INVENTION IN THE UNITED STATES TO OVERCOME CITED PATENT APPLICATION (37 C.F.R. §1.131)

We, John R. McGarvey and David Kuehr-McLaren, declare as follows:

1. We are the inventors of the invention entitled METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR SECURE DELEGATION USING PUBLIC KEY AUTHENTICATION, disclosed and claimed in U.S. Patent Application Serial No. 09/921,536 (hereinafter the '536 application), filed August 3, 2001.

2. The invention disclosed and claimed in the '536 application was conceived by us in the United States, at a date prior to June 20, 2001 which is the filing date and 35 U.S.C. §102(e) prior art date of U.S. Pat. App. Pub. No. US 2003/0018913 (hereinafter the '913 application).

3. In a final office action dated August 18, 2006, claims 1, 23-29, 31 and 32 were rejected under 35 U.S.C. §103 as being unpatentable over the '913 application in view of U.S. Pat. No. 5, 535, 276 (hereinafter the '276 patent). Additionally, claims 2, 3, 5, 7-11, 14, 15 and 30 were rejected under 35 U.S.C. §103 a being unpatentable over the '913

application in view of the '276 patent and further in view of U.S. Pat. No. 6,829,356 (hereinafter the '356 patent). Still further, claims 4, 6, 12, 13 and 20 were rejected under 35 U.S.C. §103 a being unpatentable over the '913 application in view of the '276 patent, the '356 patent and further in view of Schneier – Applied Cryptography. Still further, claims 16-19 and 21-22 were rejected under 35 U.S.C. §103 a being unpatentable over the '913 application in view of the '276 patent, the '356 patent and further in view of Menezes et al. (Handbook of Applied Cryptography).

4. We believe that we and our patent attorneys were diligent just prior to the June 20, 2001 filing date of the '913 application until the filing date of our application on August 3, 2001 based upon at least the following:

Prior to June 20, 2001, we submitted an IBM Invention Disclosure, identified as IBM RSW820000227, entitled "SECURE DELEGATION WITH EXISTING PROTOCOL FLOWS FOR PUBLIC KEY AUTHENTICATION OF THE CLIENT", which is attached hereto as exhibit A. Portions of this exhibit showing certain dates and non-relevant information have been redacted.

On February 28, 2001, Gerald R. Woods, in-house counsel for IBM, the assignee of the subject application, sent a letter to Timothy J. O'Sullivan of Myers, Bigel, Sibley & Sajovec, PA requesting that Mr. O'Sullivan prepare a patent application, assigned IBM Docket number RSW920000185US1, based on invention disclosure RSW820000227 entitled "SECURE DELEGATION WITH EXISTING PROTOCOL FLOWS FOR PUBLIC KEY AUTHENTICATION OF THE CLIENT", which is attached hereto as exhibit B. The invention disclosure is improperly identified as RSW820000277 in the *re:* line of exhibit B.

On March 8, 2001, Timothy J. O'Sullivan sent a letter to Gerald R. Woods acknowledging authorization to prepare a patent application based upon IBM's Docket number RSW920000185 US1 (corresponding to invention disclosure RSW820000227), which is attached hereto as exhibit C.

On May 18, 2001, Timothy J. O'Sullivan sent a letter to inventor John R. McGarvey enclosing an initial draft of the patent application prepared under IBM Docket number RSW9200000185 US1, which is attached hereto as exhibit D. Also attached as part of exhibit D are the first five pages of the initial draft of the draft patent application, which is entitled "METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR SECURE DELEGATION USING PUBLIC KEY AUTHENTICATION".

On July 20, 2001, John McGarvey sent an e-mail to Timothy J. O'Sullivan which included corrections to the draft patent application. The e-mail is attached hereto as exhibit E.

On July 23, 2001, Timothy J. O'Sullivan sent a letter to John R. McGarvey enclosing a final revised draft of the patent application. The letter is attached hereto as exhibit F.

On August 3, 2001 Timothy J. O'Sullivan sent a letter to Gerald R. Woods indicating that the application was filed on August 3, 2001. The letter is attached hereto as exhibit G.

5. Evidence to establish a conception date prior to June 20, 2001 for at least claims 1-7 26-28 and 30-32, can be seen on page 2 of the IBM invention disclosure RSW820000227 attached hereto as Exhibit A. In this document, "Created On" "Last Modified On" and "Submitted On" dates on page 1 have been redacted. Further, the date appearing in response to Question 1 on page 2 has been redacted. Each of the redacted dates is prior to June 20, 2001.

Evidence to establish a conception date prior to June 20, 2001 for each of the pending claims 1-32 can be seen on in the Summary section on pages 3-5 of the initial draft patent application, attached hereto as Exhibit D.

6. As a person summing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that the statements were made with the knowledge that willful false statements and the like so many are punishable by fine or imprisonment, or both, under section 1001 of title 18 of the United States code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: John Ryan McGervey

Inventor's signature: John Ryan McGervey

Date: October 23, 2006

Country of citizenship: US

Post-office address: 7133 Eastridge Drive, Apex NC 27539

Full name of second inventor: David G. Kuehr-McLaren

Inventor's signature: David G Kuehr/McLaren

Date: october 23, 2006

Country of citizenship: US

Post-office address: 205 S. Mason ST Apex, NC 27502

EXHIBIT A

Disclosure RSW8-2000-0227

Created By: John McGarvey Created On: REDACTED REDACTED REDACTED
Last Modified By: John McGarvey Last Modified On: REDACTED REDACTED

*** IBM Confidential ***

Required fields are marked with the asterisk (*) and must be filled in to complete the form.

Summary

Status	Under Evaluation
Processing Location	RSW
Functional Area	Micher: NT Suites
Attorney/Patent Professional	Gerald R Woods/Raleigh/IBM
IDT Team	Steven Miller/Raleigh/IBM; Art Francis/Raleigh/IBM; David Koehr-Mclaren/Tivoli Systems@Tivoli Systems; Allan K Edwards/Raleigh/IBM; Mark Peters/Raleigh/IBM; R Redpath/Raleigh/IBM; Scott Rich/Raleigh/IBM; Thom Haynes/Raleigh/IBM; Keith Purcell/Raleigh/IBM; Virinder Batra/Raleigh/IBM; Jay Casler/Raleigh/IBM
Submitted Date	REDACTED REDACTED REDACTED
Owning Division Select	SWG
PVT Score Calculate	To calculate a PVT score, use the 'Calculate PVT' button.
Incentive Program	
Lab	
Technology Code	

Inventors with Lotus Notes IDs

Inventors: John McGarvey/Raleigh/IBM

Inventor Name > denotes primary contact	Inventor Serial	Div/Dept	Manager Serial	Manager Name
> McGarvey, John R	165607	7JPEA	463179	Reynolds, Patrick R

Inventors without Lotus Notes IDs

IDT Selection

Main Idea

Title of disclosure (in English)

Secure Delegation with Existing Protocol Flows for Public Key Authentication of the Client

Idea of disclosure

1. Describe your invention, stating the problem solved (if appropriate), and indicating the advantages of using the invention.

Means for mutual public key authentication of a client and server are well known to practitioners of the art. The server to which the client is authenticated may act as a middle tier server for a distributed application, which accesses several back end servers on the client's behalf. It is often desirable for the middle tier server to "impersonate" the client identity when communicating with back end servers. However, the existing approaches to client authentication have a drawback in that they do not provide a secure means of client impersonation, which is sometimes called delegation.

2. How does the invention solve the problem or achieve an advantage,(a description of "the invention", including figures inline as appropriate)?

PKI authentication involves the exchange of certificates and signed "nonces". A nonce is a random number generated by one party in the exchange which is signed by the other party using its private key. The party originating the nonce can then verify the signature so as to authenticate the identity of the other party. The idea of this invention is to have the middle tier server B and each of the back end servers C, D, E, ... and so on all contribute to the generation of the nonce, by generating a prenonce token which includes a random numbers provided by each of the participating servers. This prenonce token is then reduced to a single nonce using a standard one way hash, such as MD5 or SHA. This nonce is passed in the SSL exchange, and the client signature for the nonce is obtained. The signed nonce is then used by the middle tier server B in its communications with back end servers C, D, E, ... to establish with each of these servers the authenticated client identity, so that the middle tier server can impersonate the client on each of the participating back ends.

3. If the same advantage or problem has been identified by others (inside/outside IBM), how have those others solved it and does your solution differ and why is it better?
Several approaches have been proposed for PKI authentication with delegation, but none has been widely deployed because of various drawbacks. The approach described in this invention has a big advantage in that no change is needed in the programs or data flows on the client side, and the further advantage that it should offer reasonable performance.

4. If the invention is implemented in a product or prototype, include technical details, purpose, disclosure details to others and the date of that implementation.
Not yet implemented.

***Critical Questions (Questions 1 - 7 must be answered)**

*Question 1: On what date was the invention workable REDACTED Please format the date as MM/DD/YYYY (Workable means i.e. when you know that your design will solve the problem)	
*Question 2: Is there any planned or actual publication or disclosure of your invention to anyone outside IBM?	REDACTED
If yes, Enter the name of each publication or patent and the date published below: Publication/Patent: Date Published or Issued:	REDACTED
Are you aware of any publications, products or patents that relate to this invention?	REDACTED
If yes, Enter the name of each publication or patent and the date published below: Publication/Patent: Date Published or Issued: SSL/TLS IETF RFCs, existing patents ???, on secure delegation using public key authentication	
*Question 3: Has the subject matter of the invention or a product incorporating the invention been sold, used internally in manufacturing, announced for sale, or included in a proposal?	REDACTED
Is a sale, use in manufacturing, product announcement, or proposal planned?	REDACTED
If Yes, identify the product if known and indicate the date or planned date of sale, announcements or proposal and to whom the sale, announcement or proposal has been or will be made. Product: Version/Release: Code Name: Date: To Whom: If more than one, use cut and paste and append as necessary in the field provided.	

REDACTED

RSW8-2000-0227 Secure Delegation with Existing Protocol Flows for Public Key Authentication of the Client - continued

Question 4:
Was the subject matter of your invention or a product incorporating your invention used in public (e.g. outside IBM or in the presence of non-IBMers)?
If yes, give a date: Please format the date as MM/DD/YYYY

Question 5:
Have you ever discussed your invention with others not employed at IBM?
If yes, identify individuals and date discussed. Fill in the text area with the following information: the individuals, the employer, date discussed, under CDA and CDA #

Question 6:
Was the invention, in any way, started or developed under a government contract or project?
If Yes, enter the contract number

Question 7:
Was the invention made in the course of any alliance, joint development or other contract activities?
If Yes, enter the following: Name of Alliance, Contract or Joint Developer
Contract ID number
Relationship contact name
Relationship contact E-mail
Relationship contact phone

Question 8:
Have you submitted, or are you aware of any related disclosure submission?
If Yes, please provide the title and docket or disclosure number below.
If filed, attached disclosure describing how this invention could be used, developed or implemented

Question 9:
What type of companies do you expect to compete with inventions of this type? *Check all that apply*
- Manufacturers of enterprise servers
- Manufacturers of entry servers
- Manufacturers of workstations
- Manufacturers of PCs
- Non-computer manufacturers
- Developers of operating systems
- Developers of networking software
- Developers of application software
- Integrated solution providers
- Service providers
- Other (Please specify below)

Patent Value Tool (Optional - this may be used by the inventor and attorney to assist with the evalu
Post Disclosure Text & Drawings

(Form Revised 12/17/97)

REDACTED

EXHIBIT B

Software Group
Intellectual Property Law
T81/503, P.O. Box 12195
Research Triangle Park, NC 27709

February 28, 2001

Mr. Timothy J. O'Sullivan
Myers, Bigel Sibley & Sajovec, PA
111 Corning Road
Suite 250
Cary, NC 27511

03-01-01 A09:52 IN

Ref: IBM Dockets: RSW920000185US1 (Disclosure, RSW8-2000-0277)
RSW920010046US1 (Disclosure, RSW8-2000-0202)

Title: Secure Delegation with Existing Protocol Flows for Public Key Authentication of the Client Method of Using Kerberos or other Delegated Credentials to Generate Secure Public Key Signatures

Dear Tim:

Enclosed please find materials for preparing a patent application for the above referenced dockest. We would like to have this application filed with the USPTO by June 1, 2001. The inventor involved with both applications is:

John McGarvey 919-254-7397 John McGarvey@us.ibm.com

If you have any questions, or if you need anything additional, please do not hesitate to contact me.

Thank you for your assistance in this matter.

Sincerely,

Gerald R. Woods
Attorney-IP Law
919-543-7204

GRW:ld
Enclosures

EXHIBIT C

MYERS BIGEL SIBLEY & SAJOVEC, P.A.

PATENT LAWYERS

Mailing Address:
PO Box 37428
Raleigh, NC 27627

Street Address:
Suite 250
111 Corning Road
Cary, NC 27511

(919) 854-1400
Fax (919) 854-1401

Internet
mbs@carolinapatents.com
www.carolinapatents.com

D. Randal Ayers
David D. Beatty
Mitchell S. Bigel
Sanjiri J. Biswas
Needham J. Boddie, II
James R. Cannon
Robert N. Crouse
Robert W. Glass
Scott C. Hatfield
Erin P. Madill
Karen A. Magri
Robert M. Meeks
D. Scott Moore
James D. Myers
Timothy J. O'Sullivan
Julie H. Richardson
E. Michael Sajovec
Grant J. Scott
Kenneth D. Sibley
Robert J. Smith
Elizabeth A. Sonvek
J. Michael Strickland
Richard P. Vitek*

INTELLECTUAL PROPERTY
PATENTS
TRADEMARKS
COPYRIGHTS
TRADE SECRETS

* Not Licensed in North Carolina
Licensed in California and Michigan

March 8, 2001

Gerald R. Woods, Esq.
Department T81/Building 503-3
Intellectual Property Law Department
International Business Machines Corp.
Post Office Box 12195
Research Triangle Park, NC 27709

RE: *Secure Delegation with Existing Protocol Flows for Public Key Authentication of the Client*
IBM Docket No. RSW920000185US1; Our File: 5577-236

Dear Jerry:

Thank you for your letter dated February 28, 2001, authorizing us to prepare a patent application for the above-referenced invention. Pursuant to your instructions, we will have the application prepared and filed by June 1, 2001 if possible.

Best regards.

Sincerely,

Timothy J. O'Sullivan

TJO/tb

EXHIBIT D

MYERS BIGEL SIBLEY & SAJOVEC, P.A.

PATENT LAWYERS

Mailing Address:
PO Box 37428
Raleigh, NC 27627

Street Address:
Suite 250
111 Corporate Road
Cary, NC 27511

(919) 854-1400
Fax (919) 854-1401

Internet:
mbss@carolinapatents.com
www.carolinapatents.com

D. Randal Ayers
David D. Beatty
Mitchell S. Bigel
Soroitul J. Biswas
Needham J. Boddie, II
James R. Cannon
Robert N. Crouse
Robert W. Glatz
Scott C. Hatfield
Erin P. Madill
Karen A. Magri
Robert M. Meeks
D. Scott Moore
James D. Myers
Timothy J. O'Sullivan
Julie H. Richardson
R. Michael Sajovec
Grant J. Scott
Kenneth D. Sibley
Robert J. Smith
Elizabeth A. Stanek
J. Michael Strickland
Richard P. Vitek*

INTELLECTUAL PROPERTY
PATENTS
TRADEMARKS
COPYRIGHTS
TRADE SECRETS

* Not Licensed in North Carolina
Licensed in California and Michigan

May 18, 2001

Mr. John R. McGarvey
Division 7J/Department PE9A
IBM Corporation
Post Office Box 12195
Research Triangle Park, NC 27709

VIA HAND DELIVERY

RE: *Methods, Systems and Computer Program Products for Secure Delegation Using Public Key Authentication*
IBM Docket No. RSW920000185US1; Our File: 5577-236

Dear Jerry:

Enclosed is an initial draft of a patent application directed to the above-identified invention for your review. Please provide copies to David Kuehr-McLaren. This is only a draft, so feel free to make additions, deletions, substitutions, and the like.

As you know, it is essential that the patent application, as filed, be technically accurate and complete, and that it set forth the best mode of carrying out the invention, because new matter may not be added to the descriptive portion after filing. We therefore ask that you carefully review the draft for technical accuracy and completeness, and advise us of any suggested changes or corrections. Your changes and suggestions will be carefully considered in the preparation of the final draft.

Out of an abundance of caution, we are requesting that you confirm that the proper inventive entity has been identified for the claimed invention(s). As you may be aware, inventorship is determined by the subject matter of the claimed invention. Generally stated, to be an inventor one must have made an actual contribution to the conception of the operative invention that is claimed. There may be joint inventorship even though the joint inventors (a) did not work physically together or at the same time, (b) did not make an equal contribution, or (c) did not make a contribution to the subject matter of every claim of the patent. A worker who merely carries out the instructions of another or only provides implementing devices to carry out another's ideas where the effort to do so is the exercise of one of ordinary skill is not typically an inventor. Further,

persons listed as contributing to an article describing or related to the invention are not necessarily inventors. Please feel free to call with any questions that you may have on this issue.

We would also like to point out that an inventor is required to make a Declaration when their application is filed in the U.S. Patent and Trademark Office (USPTO), acknowledging a duty to disclose information of which they are aware and which may be considered to be material to the examination of the application. "Material" in this respect is defined as information that a reasonable examiner would likely consider important in deciding whether to issue a patent. "Material" information as defined above may possibly include devices, products, publications, etc. that are similar to the invention and were publicly known before the invention, and it may also include any public disclosure, commercial use, or offer of sale of the invention more than one year prior to the filing date of the application. The USPTO encourages applicants to carefully examine 1) prior art cited in search reports of a foreign patent office in a counterpart application and 2) the closest information over which it is believed any pending claim patentably defines to ensure that any "material" information contained therein is disclosed to the USPTO.

If you are aware of any information that you believe might be considered "material," it is vitally important that it be brought to our attention as soon as possible (delays may result in a loss of patent term). We can then make a determination whether the information should be brought to the attention of the Patent and Trademark Office under the applicable rules. Please also be aware that the duty to disclose "material" information continues throughout pendency of the application, until the application issues as a patent.

You should also be aware that certain activities either in the United States or foreign countries prior to filing of the application in the United States may have a bearing on the ability to file corresponding applications in foreign countries under the applicable international treaty. These activities could include public disclosure of the invention in either written or oral form, such as published articles, patents, product announcements, and proposals, as well as through commercial exploitation of the invention, including public demonstrations, offers to sell, and sale of products incorporating the invention. If you would like to preserve your right to file corresponding foreign applications on this invention, we recommend that all such activities be avoided until the U.S. application is on file.

Pursuant to recent changes in the law, a U.S. application will be published approximately eighteen months after the earliest priority date to which the application is entitled, unless a specific non-publication request is made. Publication may in some circumstances provide additional infringement damages. There are additional fees associated with publication and third parties may submit references against the published application to the Patent Office. A request to not publish the application must be filed at the time of filing the application and must include a certification that the invention has not and will not be the subject of an application filed in a foreign country (e.g., under an

international agreement such as the PCT) that requires eighteen-month publication. If you later wish to file an application in a foreign country, we must promptly rescind the non-publication request to avoid abandonment of the application. A request to withhold publication will incur additional fees and expenses. If you would like for us to file a request to prevent publication of the application, please inform us immediately in writing. We will not request non-publication of the application unless you instruct us to do so.

Once you have had an opportunity to review the draft application, please let me know as soon as possible. As always, please feel free to call us with any questions that you may have.

We are to file this by **June 1, 2001** and would, therefore, appreciate any comments by **May 25, 2001.**

Best regards.

Sincerely,

Timothy J. O'Sullivan

TJO/tb

Attorney Docket No.: 5577-236

METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR SECURE DELEGATION USING PUBLIC KEY AUTHENTICATION

Field of the Invention

The present invention relates to authentication and more particularly to authentication of a client when delegation is utilized to access a server.

Background of the Invention

Networked computer applications are often deployed using a "tiered" model. In this model, the originator of a request for a unit of work (also referred to as a "principal") typically initiates that work via a client program (first tier), which then communicates to a web server, or similar second tier server (also referred to as a middle-tier server), which itself communicates, on behalf of the request originator, to other middle-tier servers and/or to third or fourth tier servers such as database servers or other resource managers. When the request is processed by the resource managers, they, typically, evaluate whether the request originator has been authenticated and whether they are authorized to perform the unit of work. The resource managers, typically, also record access by the originator of the request in appropriate audit logs.

Such a tiered approach to networked applications may create a need for the secure propagation of security credentials of the request originator through each of the tiers of the application. In such propagation of secure credentials, the request originator delegates to the middle-tier servers the authority to access other servers

on their behalf. Thus, the secure propagation of the credentials of the request originator (the requesting "principal") may be referred to as "delegation" or "impersonation."

One conventional approach for asynchronous message based authentication is to create a digital signature for the message. The digital signature is based on a public/private key pair. An example of such a digital signature approach to authentication is Public Key Infrastructure (PKI) authentication. In PKI, typically, a nonce, which may, for example, be a 60 bit random number, is generated by a party, such as a server, and provided to the client. The client signs the nonce with its digital signature and returns the signed nonce to the server. Typically, the server evaluates the digital signature of the client by decrypting the signed nonce with the public key of the client, which may be obtained from a certificate associated with the client, and comparing the decrypted nonce to the nonce originally sent. If the nonces are the same, the signature is authentic. In such a manner, the server may be assured of the authenticity of the client.

One difficulty with such a PKI authentication procedure is that it may be difficult to provided delegation of client authentication in certain circumstances. For example, a request from a principal through a client may pass through a middle-tier server which, in response to the request, accesses multiple third or fourth tier servers (also referred to as back-end servers). In such a case, the middle-tier server may need to authenticate the principal or the client to multiple back-end servers. Such a delegation of authentication may difficult in light of the multiple servers for which the client may need authentication.

Summary of the Invention

Embodiments of the present invention provide methods, systems and computer program products for a middle-tier server to impersonate a client to a plurality of servers. A common nonce associated with each of the plurality of servers is obtained and the common nonce to the client. The common nonce signed by the client is received at the middle-tier server and provided as a signature

for transactions from the client to the plurality of servers so as to authenticate the client to the plurality of servers.

In further embodiments of the present invention, obtaining a common nonce is provided by generating a common nonce based on information obtained from each of the plurality of servers. In such embodiments, generating the common nonce may be accomplished by obtaining pre-nonce contributions from the plurality of servers, combining the pre-nonce contributions to provide a single pre-nonce token and providing the common nonce based on the pre-nonce token. The common nonce may be provided by reducing the pre-nonce token to provide the common nonce. Furthermore, the pre-nonce contributions may be combined to provide a single pre-nonce token by concatenating the pre-nonce contributions. Also, the pre-nonce token may be reduced to provide the common nonce by hashing the pre-nonce token utilizing a one-way hash function so as to provide the common nonce.

In additional embodiments of the present invention, obtaining pre-nonce contributions may be provided by requesting a pre-nonce contribution from each of the plurality of servers and receiving the pre-nonce contributions from the plurality of servers. The request for a pre-nonce contribution may be provided by sending authenticated requests to the plurality of servers. Additionally, the authenticated requests may be sent to the plurality of servers may be encrypted. The authenticated request may include at least one of an identification of a source of the request, a time stamp and a random number.

In still further embodiments of the present invention, the pre-nonce contributions include at least one of an identification of a server of the plurality of servers and a random number. Furthermore, the pre-nonce contributions may be signed with a signature corresponding to a server from which the pre-nonce contribution was obtained. In such embodiments, the signatures may be incorporated in the pre-nonce token.

In yet further embodiments of the present invention, the pre-nonce contributions are signed with a signature corresponding to a server from which the pre-nonce contribution was obtained. In such embodiments, the signatures of the

pre-nonce contributions are authenticated and the pre-nonce contributions for which the digital signature are not authentic are rejected.

In still further embodiments of the present invention, a transaction identification is received from a trusted server of the plurality of servers and the transaction identification associated with the common nonce. Use of the common nonce may be tracked based on the transaction identification.

In additional embodiments of the present invention, an expiration time is associated with a pre-nonce contribution and it is determined if the pre-nonce contribution has expired based on its associated expiration time. In such embodiments, the common nonce may be received at a server of the plurality of servers and a pre-nonce contribution associated with the received common nonce is determined. The received common nonce is accepted if the associated pre-nonce contribution has not expired.

In yet additional embodiments of the present invention, at least one of the plurality of servers receives a client certificate, determines if the client certificate is trusted and indicates that the client is not authenticated if the client certificate is not trusted. Furthermore, the signed common nonce and a client certificate may be received and it is determined if the signature of the signed common nonce corresponds to a signature of the client certificate. The client is not authenticated if the signature of the signed common nonce does not correspond to the signature of the client certificate. The signed common nonce, the common nonce and the pre-nonce token may also be received and the received pre-nonce token hashed. The hashed pre-nonce token is compared to the common nonce and the client is not authenticated if the hashed pre-nonce token is different from the common nonce. The pre-nonce token may also be received at one of the plurality of servers ad it determined if the pre-nonce token includes a random number associated with the receiving server. The client is not authenticated if the pre-nonce token does not include the random number associated with the receiving server. Additionally, an expiration may be associated with the random number associated with the at least one of the plurality of servers and the client is not authenticated if the pre-nonce

token does not include a random number associated with the at least one of the plurality of servers which has not expired.

In still further embodiments of the present invention, the common nonce is obtained by obtaining the common nonce from a party trusted by the middle-tier server and the plurality of servers. The common nonce is signed by the trusted party. The signature of the common nonce is verified the signature of the trusted party. In further embodiments, at least one of the plurality of servers receives a client certificate and determines if the client certificate is trusted The client is not authenticated if the client certificate is not trusted. The signed common nonce and a client certificate may also be received and it determined if the signature of the signed common nonce corresponds to a signature of the client certificate. The client is not authenticated if the signature of the signed common nonce does not correspond to the signature of the client certificate.

As will further be appreciated by those of skill in the art, while described above primarily with reference to method aspects, the present invention may be embodied as methods, apparatus/systems and/or computer program products.

Brief Description of the Drawings

Figure 1A is a block diagram illustrating a system incorporating embodiments of the present invention;

Figure 1B is a block diagram illustrating a system incorporating alternative embodiments of the present invention;

Figure 2 is a block diagram of a data processing system according to embodiments of the present invention;

Figure 3 is a more detailed block diagram of a data processing system according to embodiments of the present invention;

Figure 4 is a flowchart illustrating operations of a middle-tier server according to embodiments of the present invention;

Figure 5 is a flowchart illustrating operations for common nonce generation according to embodiments of the present invention;

EXHIBIT E

Tim O'Sullivan

From: John McGarvey [mcgarvey@us.ibm.com]
Sent: Friday, July 20, 2001 2:19 PM
To: Tim O'Sullivan
Cc: David Kuehr-McLaren
Subject: RE: Re disclosure: Attorney docket 5577-236

Tim,

I finally got a chance to comb through your writeup. I think it is very good, and these changes are only little additions for clarity.

P1, end of line 15, add: This means of authenticating the client is used in a variety of computer protocols, including Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

line 29: servers is obtained, and then the common nonce is sent to the client. The common nonce is digitally signed by the client, and is received ...

P4 line 21 The signed common nonce and the pre-nonce token may ...

line 25: ... plurality of servers, where it is determined if the pre-nonce token includes a pre-nonce contribution from the receiving server. For example, if such contributions are digitally signed before they are contributed, the receiving server may verify its signature. The client is not authenticated ...

Figure 1A, figure 1B: Here in the figures, where we indicate "signed nonce" as passing from the middle tier server to the back end server, we may instead want to use the phrase "authenticated request packet", with explanations that this includes the request itself, the pre-nonce token, the client certificate, and the signed nonce. It may also be useful to show that Server 20 could, optionally, forward a request packet with a request, pre-nonce token, client certificate, and signed nonce, to one of the other servers (22 or 24 in the diagram). This shows the idea of further downstream chaining of delegated authority.

Figure 8: block 810 has a typo: Sigature should be signature.

That's all the changes I have to recommend. Sorry it took so long.

Regards,
John

EXHIBIT F

MYERS BIGEL SIBLEY & SAJOVEC, P.A.

PATENT LAWYERS

Mailing Address:
PO Box 37428
Raleigh, NC 27627

Street Address:
Suite 290
111 Cascade Road
Cary, NC 27511

(919) 854-1400
Fax (919) 854-1401

Internet
mbsi@carolinapatents.com
www.carolinapatents.com

D. Randal Ayers
David D. Beatty
Mitchell S. Bigel
Soroush J. Bigvas
Needham J. Boddie, II
James R. Carmon
Robert N. Crouse
Robert W. Glass

Scott C. Hatfield
Erin P. Merrill
Karen A. Mogel
Robert M. Meeks
D. Scott Moore
James D. Myers
Timothy J. O'Sullivan

Julie H. Richardson
E Michael Sajovec
Grant J. Scott
Kenneth D. Sibley
Robert J. Smith
Elizabeth A. Stanek
J. Michael Strickland
Richard P. Vitek*

INTELLECTUAL PROPERTY
PATENTS
TRADEMARKS
COPYRIGHTS
TRADE SECRETS

*Not Licensed in North Carolina
Licensed in California and Michigan

July 23, 2001

Mr. John R. McGarvey
Division 7J/Department PE9A
IBM Corporation
Post Office Box 12195
Research Triangle Park, NC 27709

RE: *Methods, Systems and Computer Program Products for Secure Delegation Using Public Key Authentication*
IBM Docket No. RSW920000185US1; Our File: 5577-236

Dear John:

Enclosed please find a revised, final draft of the patent application and the drawings directed to the above-identified invention. Also enclosed are the Declaration and Power of Attorney and the Assignment for confirming ownership in International Business Machines Corporation. We appreciate your assistance in coordinating the review and execution by the other inventor, David Kuehr-McLaren.

As previously noted, it is essential that the patent application, as filed, be technically accurate and complete, and that it set forth the best mode of carrying out the invention. If the application is fully satisfactory, then you should read and then execute the Declaration and Power of Attorney attached to the application. Please note that the application must be complete in all respects, *i.e.*, all changes must be made before the Declaration and Power of Attorney is executed. In the event any changes are made, each such change to the patent application must be initialed and dated.

Please return all original, executed documents as soon as possible for filing with the United States Patent Office.

Sincerely,

Timothy J. O'Sullivan

TJO/tb
Enclosures

EXHIBIT G

MYERS BIGEL SIBLEY & SAJOVEC, P.A.

PATENT LAWYERS

MAILING ADDRESS:
PO Box 37428
Raleigh, NC 27627

STREET ADDRESS:
Suite 200
111 Cornelia Road
Cary, NC 27511

(919) 854-1400
Fax (919) 854-1401

INTERNET:
mbas@carolinapatents.com
www.carolinapatents.com

D. Randal Ayers
David D. Beatty
Mitchell S. Bigel
Sorojini J. Biswas
Needham J. Boddie, II
James R. Cannon
Robert N. Crouse
Robert W. Glatz
Scott C. Hatfield
Erin P. Madill
Karen A. Magri
Robert M. Meeks
D. Scott Moore
James D. Myers
Timothy J. O'Sullivan
Julie H. Richardson
E Michael Sajovec
Grant J. Scott
Kenneth D. Sibley
Robert J. Smith
Elizabeth A. Stanek
J. Michael Strickland
Richard P. Vitek*

INTELLECTUAL PROPERTY
PATENTS
TRADEMARKS
COPYRIGHTS
TRADE SECRETS

* Not Licensed in North Carolina
Licensed in California and Michigan

August 3, 2001

Gerald R. Woods, Esq.
Department T81/Building 503-3
Intellectual Property Law Department
International Business Machines Corp.
Post Office Box 12195
Research Triangle Park, NC 27709

RE: McGarvey, et al. *Methods, Systems And Computer Program Products For Secure Delegation Using Public Key Authentication*
IBM Docket No. RSW920000185US1; Our File: 5577-236

Dear Jerry:

The above-referenced application (copy enclosed) was filed in the United States Patent and Trademark Office by the express mail procedure on August 3, 2001, and should receive this date as the official filing date. We have also enclosed a diskette containing the application in WordPerfect 6.0 format and the drawings in VISIO 4.0 format.

If you have any questions or comments please feel free to contact us at your convenience. Thank you again for the opportunity to assist you in this matter.

Best regards.

Sincerely,

Timothy J. O'Sullivan

TJO/tb
Enclosures